Eisenstein's Irreducibility Criterion

We present Eisenstein's Irreducibility Criterion which gives a sufficient condition for a polynomial over a unique factorization domain to be irreducible. This is followed by a famous application: for any prime p, the polynomial

$$\phi(X) = X^{p-1} + X^{p-2} + \ldots + 1$$

is irreducible in $\mathbb{Z}[X]$. We conclude by explaining why it is possible to then deduce that $\phi(X)$ is irreducible in $\mathbb{Q}[X]$.

Theorem 1 (Eisenstein's Irreducibility Criterion
)**.** *Let R be a unique factorization domain. Suppose*

$$0 \neq f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$$

is a monic polynomial in $R[X]$, and $p \in R$ is a prime such that $p|a_{n-1}, \ldots, a_0$ but $p^2 \nmid a_0$. Then $f(X)$ is irreducible.

Proof. Suppose not, so

$$f(X) = (X^r + b_{r-1}X^{r-1} + \ldots + b_0)(X^s + c_{s-1}X^{s-1} + \ldots + c_0)$$

with $0 < r, s < n$. Take i least such that $p \nmid b_i$ (where we allow the case $i = r$ and $b_r = 1$), and j least such that $p \nmid c_j$ (where we allow the case $j = s$ and $c_s = 1$). Now the $(i+j)$th coefficient a_{i+j} of the product is

$$a_{i+j} = b_i c_j + (b_{i-1}c_{j+1} + \ldots) + (b_{i+1}c_{j-1} + \ldots)$$

and so is a sum of $b_i c_j$ and terms divisible by p. As $p \nmid b_i c_j$, $p \nmid a_{i+j}$. But $p^2 \nmid a_0 = b_0 c_0$ and so p cannot divide both b_0 and c_0, and so either $i = 0$ or $j = 0$ and so $i + j < n$. So we contradict $p|a_{i+j}$. $\square$

Corollary 2. *If p is a prime then the polynomial*

$$\phi(X) = X^{p-1} + X^{p-2} + \ldots + 1$$

is irreducible in $\mathbb{Z}[X]$.

Proof. $\phi(X)$ is irreducible iff $\phi(Y+1)$ is irreducible. But

$$\begin{aligned}
\phi(Y+1) &= (Y+1)^{p-1} + (Y+1)^{p-2} + \ldots + 1 \\
&= \sum_{i=0}^{p-1} \left(\binom{p-1}{i} + \binom{p-2}{i-1} + \ldots + \binom{p-1-i}{0} \right) Y^{p-1-i} \\
&= \sum_{i=0}^{p-1} \binom{p}{i} Y^{p-1-i}.
\end{aligned}$$

So p divides all the coefficients but the first and p^2 does not divide the last and so by Eisenstein, $\phi(Y+1)$ is irreducible. $\square$

Proposition 3. *Let R be a unique factorization domain with field of fractions F. Suppose $f(X) \in R[X]$ is such that f factorizes in $F[X]$ into a product of two polynomials of lower degree. Then it does so in $R[X]$.*

Proof. Suppose $f \in R[X]$ and $f = gh$ for some $g, h \in F[X]$. Write $f = a\tilde{f}$, $g = \frac{b}{c}\tilde{g}$, $h = \frac{d}{e}\tilde{h}$ where $\tilde{f}, \tilde{g}, \tilde{h} \in R[X]$ are primitive. Then $a\tilde{f} = \frac{bd}{ce}\tilde{g}\tilde{h}$ so $ace\tilde{f} = bd\tilde{g}\tilde{h}$. But $\tilde{f}$ and $\tilde{g}\tilde{h}$ are primitive (by Gauss) and so $bd = uace$ for some unit $u \in R$. Then $\tilde{f} = u\tilde{g}\tilde{h}$ and so $f = (ua\tilde{g})\tilde{h}$ is factorized in $R[X]$. $\square$

Note that we say "it does so" in the statement of this proposition to take account of the possibility of factorization in $R[X]$ which is irrelevant from the point of view of $F[X]$. For example, $2X^2 + 2X + 2 = 2(X^2 + X + 1)$ factorizes in $\mathbb{Z}[X]$ but it is irreducible in $\mathbb{Q}[X]$ (2 is a unit there).

Now, suppose we have a polynomial $f(X) \in \mathbb{Q}[X]$ and we want to know whether or not it is irreducible. Write $f(X) = \frac{r}{s}\tilde{f}(X)$ with $\tilde{f}$ primitive in $\mathbb{Z}[X]$. Then f is irreducible in $\mathbb{Q}[X]$ iff $\tilde{f}$ is irreducible in $\mathbb{Q}[X]$ iff $\tilde{f}$ is irreducible in $\mathbb{Z}[X]$.

Corollary 4. *If p is a prime then the polynomial*

$$\phi(X) = X^{p-1} + X^{p-2} + \ldots + 1$$

is irreducible in $\mathbb{Q}[X]$.